## Batch Information:

* **Batch Start Date:** 2025-08-04
* **Batch Name:** WiproNGA\_DWS\_B5\_25VID2550
* **First Name:** Manojit Kumar Das
* **User ID:** 34873
* **Batch ID:** B5-25VID2550

ASSIGNMENTS

* **Interactive and Non-Interactive Applications**
* **Required and Available App assignments**
* **Groups, Dynamic queries, Users**
* **Process Flow for an Application on Windows client via IME service. (From Polling to detection, to installation , to detection and toast notifications as success/failure)**
* **Registries with respect to LOB and Win32Apps**
* **Specific Registries with Application GUID which give you the status of Installation/Uninstallation.**
* **Log File locations & Company Portal**
* **How to Sync once app assignments are done. (Intune Device Sync/ Company Portal Local side Sync)**

**--------------------------------------------------------------------------------------------------------------------------**

# Interactive and Non-Interactive Applications.

In the context of **Application Packaging** and **Enterprise Deployment**, understanding whether an application is *interactive* or *non-interactive* is critical. It affects how the application is **installed**, **configured**, and **deployed silently** in large-scale enterprise environments using tools like **SCCM**, **Intune**, or **GPO**.

## What are Interactive Applications? Definition:

Interactive applications are those that **require user interaction** during installation or runtime. This includes clicking "Next", selecting options, entering license keys, accepting agreements, or making configuration choices.

## Common Characteristics:

* + Show GUI windows, dialogs, or prompts.
  + Require human input.
  + Can’t be installed silently without modifications.
  + May block automation if not handled properly.

## Examples:

* + Setup.exe that asks for install location, license key, or user preferences.
  + Applications that pop up configuration windows post-installation.
  + Installers that require selecting features manually.

## Handling in Packaging:

* + Must be converted to **non-interactive** (silent) using switches like /silent,

/quiet, /qn (for MSI), or by creating a response/answer file.

* + May need scripting or transform files (.MST) to suppress dialogs.

## What are Non-Interactive Applications?

**Definition**:

Non-interactive applications are designed to run without requiring **any user interaction**. They can be installed silently and are ideal for automated deployments across multiple systems.

## Common Characteristics:

* + Fully silent or unattended installation.
  + Accepts default settings or pre-configured options.
  + Compatible with deployment tools (like SCCM, Intune).
  + Don’t show GUI prompts.

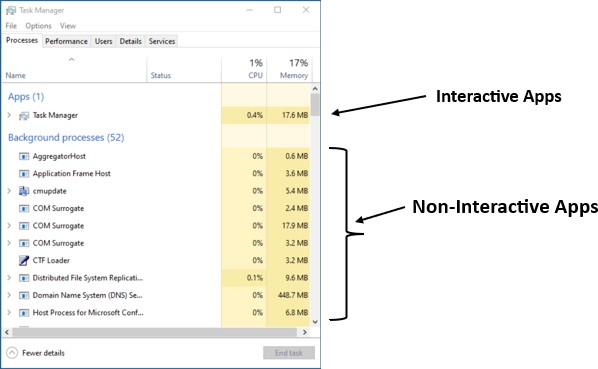
## Examples:

* + MSI installers with /qn flag (quiet, no UI).
  + EXE installers with proper silent switches like /S, /quiet, /norestart.
  + Custom-packaged applications prepared using tools like **AdminStudio**, **Advanced Installer**, or **PSADT** (PowerShell App Deployment Toolkit).

## Handling in Packaging:

* + Preferred format for deployment.
  + Easy to script, schedule, or push through automation tools.
  + Fewer chances of deployment failure due to human error.
* **Why This Matters?**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Interactive Apps** | **Non-Interactive Apps** |
| User Involvement | Required | Not required |
| Automation Compatibility | Poor | Excellent |
| Deployment Speed | Slower | Faster |
| Risk of Human Error | Higher | Lower |
| Suitable for SCCM/Intune | Needs conversion | Directly deployable |



# Required and Available App assignments.

## What are App Assignments?

When deploying applications (especially via tools like **Microsoft Intune**, **SCCM**, etc.), you assign apps to user groups or device groups. These assignments define **how and when** the app gets installed on the target systems.

App assignments are typically categorized into two types:

## Required

1. **Available**
2. **Required App Assignment:**

## Definition:

In a "Required" assignment, the app is **automatically pushed and installed**

on the user’s device or system **without user interaction**.

## Key Characteristics:

* + - Installation is **mandatory**.
    - It happens **as soon as possible** (based on deployment schedule).
    - The user **cannot cancel or postpone** it.
    - Often used for **critical business apps** like antivirus, VPN client, office tools, etc.
    - Admins can set a **specific deadline** for the installation.
    - App will **reinstall automatically** if it's uninstalled.
  + **Real-World Example:** You assign Microsoft Teams as a required app to all corporate laptops. Every device will have it installed silently in the background without needing user approval.

1. **Available App Assignment:**

## Definition:

In an "Available" assignment, the app is **optional** and shown in a **company portal** (like Intune Company Portal) where users can **choose to install it** themselves.

## Key Characteristics:

* + - Installation is **user-initiated**.
    - App is **not forced** onto the device.
    - Good for **optional tools** (e.g., PDF editors, development tools, training apps).
    - Offers **self-service flexibility**.
    - Reduces unwanted installations and user complaints.
  + **Real-World Example:** You assign Adobe Reader as an available app. Users who need it can open the Company Portal and click "Install".
  + **When to Use What?**

|  |  |
| --- | --- |
| **Situation** | **Recommended Assignment Type** |
| Business-critical or security apps | Required |
| Optional tools or utilities | Available |
| Testing apps in a controlled group | Available |
| Rollout with guaranteed presence | Required |

# Groups, Dynamic queries, Users.

## Users

* + - A **user** is anyone who logs into a system (e.g., employee).
    - Two types:
      * **Local User** – Exists only on one PC.
      * **Domain User** – Managed in Active Directory, can log in on any domain-joined PC.
    - Used in packaging for:
      * Per-user settings
      * Active Setup
      * Logon scripts

## Groups

* + - A **group** is a collection of users to manage permissions and deployments easily.
    - Types:
      * **Security Group** – Controls access to apps/files.
      * **Distribution Group** – For sending emails (not used for access).
    - Helps in:
      * Targeting software to specific teams (e.g., HR, IT)
      * Applying GPO or logon scripts

## Dynamic Queries

* + - Rules used to **auto-fill groups or collections** based on user/device properties.
    - Used in tools like **SCCM** or **Azure AD**.
    - Example: Automatically include all laptops with Windows 11 and HR users in a group.
    - Saves time – no need to add users/devices manually.

# Process Flow for an Application on Windows client via IME service. (From Polling to detection, to installation , to detection and toast notifications as success/failure).

In a Microsoft Intune-managed environment, the **Intune Management Extension (IME)** plays a crucial role in delivering **Win32 apps**, **PowerShell scripts**, and other custom configurations to Windows clients. The process flow—from polling to detection, installation, and notification—is vital for ensuring reliable app deployment and user communication.

## Polling Phase

* + The IME service regularly **polls Intune service** for new instructions or targeted applications.
  + Default polling frequency is **every 60 minutes** (can vary slightly).
  + IME contacts **Microsoft Intune cloud service** to:
    - Check for new app assignments.
    - Update status for previous installations.
    - Retrieve scripts, Win32 apps, or configurations.

## Detection Phase

* + After receiving app deployment instructions, IME first checks whether the application **already exists** on the device.
  + This is done using a **Detection Rule** configured during packaging (e.g., file existence, registry key, MSI GUID, etc.).
  + If the detection rule returns **“App is already installed,”** IME will **skip installation**.
  + If **not detected**, it proceeds to the installation phase.

## Installation Phase

* + IME downloads the **app payload** (like a .intunewin package) from Intune’s storage.
  + App is installed silently using:
    - System context (default)
    - Custom install command (like install.cmd or .exe /silent)

## Post-Installation Detection

* + After installation, **IME re-runs the detection rule** to confirm successful installation.
  + If detection rule **now returns “App is installed” → Success**.
  + If not → installation is **marked as failed**.
  + Results are reported back to **Intune portal** for admin visibility.

## Toast Notifications (User Experience)

* + Based on the app deployment configuration, the end user may receive:
    - **Success notification**: App installed successfully.
    - **Failure notification**: Installation failed with error code.
  + These toast notifications help improve transparency and user trust in managed device environments.
  + Admins can customize whether notifications appear or not.

# Registries with respect to LOB and Win32Apps.

## What is the Windows Registry?

The **Windows Registry** is a hierarchical database used by the Windows operating system to store configuration settings and options for:

* + The operating system
  + Installed applications
  + System hardware
  + User profiles

It contains keys and values that applications can read from or write to during installation, configuration, and runtime.

1. **LOB Apps (Line-of-Business Applications):**

**Definition:** LOB apps are custom-built or internal-use applications used within an organization. These are often packaged and deployed via tools like **Microsoft Intune (Endpoint Manager)**.

## Registry behavior:

* + Typically installed **per-user** or **per-device**, depending on the deployment configuration.
  + Uses HKCU if deployed to **user context**.
  + Uses HKLM if deployed to **device/system context**.
  + Registry entries might store:
    - Licensing information
    - Configuration settings
    - Logging preferences
    - App versioning data

1. **Win32Apps:**

**Definition:** Win32Apps are classic Windows desktop applications (typically .EXE or .MSI) deployed via **Intune (Endpoint Manager)** using Win32 App deployment model.

## Registry behavior:

* + Mostly installed in **system context**, using **HKLM**.
  + May also use HKCU if app is user-specific or modifies user preferences.
  + Registry entries can include:
    - Install state
    - Version tracking
    - App configurations
    - Installer logs

## Intune also uses registry checks for:

* + **Detection rules** (e.g., to detect if an app is installed)
  + **Requirement rules**
  + **Remediation scripts**

# Specific Registries with Application GUID which give you the status of Installation/Uninstallation.

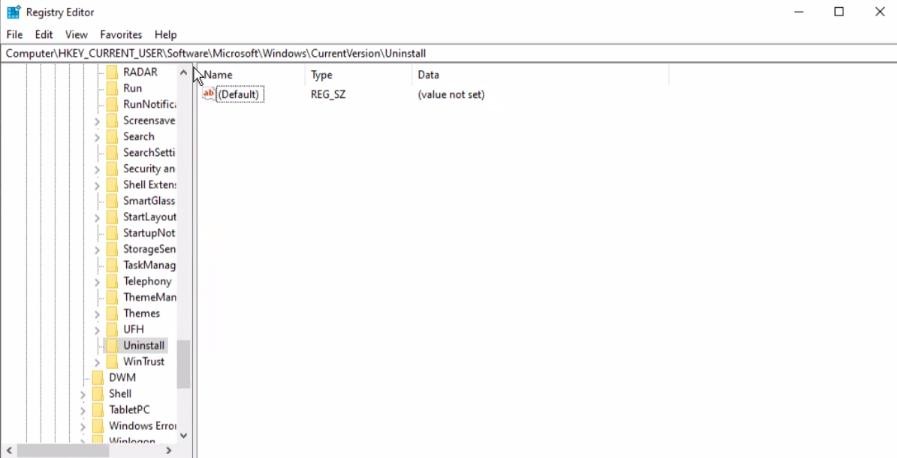
## Checking Installation/Uninstallation Status & Finding Application GUIDs via Registry:

To verify the installation or uninstallation status of an application and to locate its GUID (Product Code), the Windows Registry can be used. The relevant registry paths are:

## Per-machine-installations:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

## Per-user-installations:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Each of these keys contains subkeys for installed applications. The subkey may use the application's name or a unique identifier such as a GUID.

## Locating the GUID (Product Code)

* + Inside the uninstall registry path, subkeys represent individual applications.
  + The GUID is a 32-character hexadecimal string (e.g., {80890A63-01AA- 40D3-A2E9-B3E214735151}).
  + It uniquely identifies the application and is essential for uninstall operations.

## Using the GUID to Uninstall

* + The msiexec command utilizes the GUID to perform uninstallations:

*msiexec.exe /x {Product-GUID} /QN /L\*V "C:\Client-uninstall\desktop- uninstall.log"*

* + - /x – Uninstall the application.
    - /QN – Silent mode (no UI).
    - /L\*V – Logs the process to the specified path.

# Log File locations & company portal.

Event logs are vital records that capture system and application activities. They help in **monitoring**, **debugging**, and **analyzing** issues by providing detailed insights into what happens on a system.

## Key Aspects of Event Logs

* + **Timestamps:** Show the exact time an event occurred — essential for tracing event sequences.
  + **Event Types:** Classify events as *Error*, *Warning*, *Information*, or *Audit*

(Success/Failure) for better understanding.

* + **Severity Levels:** Indicate the impact of an event, such as Critical, Error, Warning, or Informational.
  + **Descriptions:** Give in-depth details including error codes, affected components, and user actions.
  + **EventIDs:** Unique identifiers assigned to events, making them easier to search and analyze.
  + **Categories:** Logs are grouped into types like:
    - **System Logs**
    - **Application Logs**
    - **Security Logs**
    - **Audit Logs**

# How to Sync once app assignments are done. (Intune Device Sync/ Company Portal Local side Sync).

## Sync Using the Company Portal App

This is the most common method used by end users across Windows and Android devices.

Steps:

* + Launch the Company Portal app on your device.
  + Navigate to Settings.
  + Tap or click on Sync.
  + Wait for the synchronization process to complete.

## Sync from the Intune Admin Center

This method is typically used by IT administrators to remotely trigger a sync for a device.

## Steps:

* + Sign in to the **Microsoft Intune Admin Center**.
  + Navigate to **Devices > All devices**.
  + Select the specific device you want to sync.
  + Under the **Overview** tab, click on **Sync**.
  + Confirm by selecting **Yes** when prompted.

## Sync from Windows Settings (Work or School Account)

Available on Windows 10/11 devices linked to a work or school account.

## Steps:

* + Open the **Settings** app on the Windows device.

## Go to Accounts > Access work or school.

* + Select the connected **work account**, then click on **Info**.
  + Click **Sync** to manually trigger the device check-in with Intune.

## Sync from Taskbar or Start Menu (Windows Only)

Quick access method via the Company Portal icon on Windows.

## Steps:

* + Locate the **Company Portal** icon in the system tray (taskbar) or **Start Menu**.
  + **Right-click** the icon.
  + Select **Sync this device**.

